

CLAIMS

1 1. A hybrid stream cipher operating within a computing device, comprising:
2 a first software routine to divide incoming plain text into variable-sized blocks; and
3 a second software routine to convert the plain text into cipher text based on an encryption
4 key and an internal identifier.

1 2. The hybrid stream cipher of claim 1, wherein the first software routine produces
2 the variable-sized blocks based on the encryption key, the internal identifier and an output of a
3 first non-linear function.

1 3. The hybrid cipher of claim 2, wherein each current block of the plain text is
2 determined by (i) producing a pseudo-random sequence using a second non-linear function
3 including the encryption key, the internal identifier and the output of the first non-linear function
4 as inputs and (ii) accessing contents of the pseudo-random sequence as a number of data
5 elements of the plain text forming the current block.

1 4. The hybrid cipher of claim 1, wherein the second software routine further
2 performs a first shuffling operation on an internal state of a computing device based on the
3 encryption key so that a single bit modification of the encryption key requires complete
4 recalculation of the internal state of the computing device.

1 5. The hybrid cipher of claim 4, wherein the second software routine further
2 performs a second shuffling operation on the internal state of the computing device based on at
3 least the internal identifier to mitigate a likelihood of prediction of the internal state of the
4 computing device upon knowledge of the encryption key.

1 6. The hybrid cipher of claim 1 further comprising:
2 a third software routine to determine if a plurality of random data elements are to be
3 distributed within the cipher text.

1 7. The hybrid cipher of claim 6, wherein the third software routine determines an
2 amount of random data elements distributed within the cipher text is programmable based on a
3 percentage value entered by a user, or set based on the encryption key and internal identifier and
4 the internal state of the hybrid stream cipher.

1 8. The hybrid cipher of claim 6, wherein the third software routine determines an
2 amount of random data elements distributed within the cipher text is set based on the encryption
3 key, the internal identifier and the internal state of the computing device.

1 9. The hybrid cipher of claim 6, wherein the plurality of random data elements are
2 produced by a pseudo-random generator.

1 10. The hybrid cipher of claim 1 further comprising a third software routine to map
2 the input plain text before undergoing operations of the second software routine to avoid
3 statistics of the plain text from reflecting an internal state of the computing device.

1 11. The hybrid cipher of claim 1 further comprising a third software routine to
2 produce an output stream based on a mixing of the cipher text, a plurality of random data
3 elements and a hash digest of a portion of the output stream.

1 12. The hybrid cipher of claim 1 further comprising a third software routine to
2 distribute one of a digital signature and a watermark in the cipher text in order to detect
3 modification.

1 13. The hybrid cipher of claim 12 further comprising a fourth software routine to
2 calculate and distribute a hash of the cipher text, a plurality of the random data elements and the
3 digital signature within an output stream.

1 14. The hybrid cipher of claim 1 further comprising a third software routine to
2 convert cipher text to plain text based on a table lookup using an array having data elements that
3 are permuted to correspond to an inverse of an array of an internal state of the computing device.

1 15. A computing device comprising:
2 a memory; and
3 logic to perform a stream cipher operation using an encryption key on input data
4 segmented in random sized blocks.

1 16. The computing device of claim 15, wherein the stream cipher operation involves
2 encryption.

1 17. The computing device of claim 15, wherein the logic is an integrated circuit.

1 18. The computing device of claim 15, wherein the hybrid stream cipher processed by
2 the logic produces random-sized blocks of the input data based on an encryption key, the unique
3 internal identifier and an output of a first non-linear function.

1 19. The computing device of claim 18, wherein each block of the plain text is
determined by the hybrid stream cipher (i) producing a pseudo-random sequence using a second
non-linear function including the encryption key, the internal identifier and the output of the first
non-linear function as inputs and (ii) accessing contents of the pseudo-random sequence as a
number of data elements of the plain text forming the current block.

1 20. The computing device of claim 15, wherein the computing device is a smart card.

1 21. The computing device of claim 15, wherein the computing device is a node
2 coupled to a network and alternatively a router.

1 22. The computing device of claim 15, wherein the logic of the computing device is
2 an operating system.

1 23. The computing device of claim 15, wherein the computing device is a wireless
2 device.

1 24. The computing device of claim 15, wherein the memory of the computing device
2 is a portable storage medium that, only when in communication with the logic, enables the logic
3 to perform the stream cipher operation on the random-sized blocks.

1 25. A method for decrypting input data using a combination of stream cipher and
2 block cipher functionality, comprising:

3 receiving as input a cipher text, a decryption key, a percentage of random data and a
4 unique internal identifier; and
5 reiteratively decrypting blocks of the cipher text using the decryption key, the
6 percentage of random data and the unique internal identifier to recover corresponding blocks of
7 plain text.

1 26. The method of claim 25 further comprising verifying a digital signature
2 distributed in the cipher text and aborting decryption if one bit of the plain text has been
3 changed.

1 27. A mechanism for securely selling digital content, comprising:
2 assigning a unique internal identifier to each user;
3 receiving a request from a user for a download of the digital content;
4 encrypting the digital content using a hybrid stream cipher, the hybrid stream cipher
5 using as inputs the internal identifier, an encryption key, and a percentage of random data value
6 to control conversion of the digital content into an encrypted digital content; and
7 transmitting the encrypted digital content to the user.

1 28. The mechanism of claim 27 includes a copyright in one of a plain text form, an
2 image or an icon to operate as a digital signature, that is needed for decrypting the digital content
3 and allowing the digital content to be uniquely sold to a particular user.

1 29. The mechanism of claim 27, wherein the digital content is software that is placed
2 on a removable media or downloaded on-line.